
Hridesh Rajan and Wensheng Zhang

Broad Problem
- Sensor networks often used in hostile settings, need to secure these networks
- Specifying and verifying new protocols is harder
- Issues: unboundedness, topological issues, intruder behavior

Specific Problem #1: Verification from Specification is not enough
- Specialized knowledge in specification language required
- No guarantee that the implementation is implementing the verified specification of the protocol
- Approach: Extract verifiable models from protocol implementations

Specific Problem #2: Undecidability of the Problem
- State explosion in model checking:
  - Unbounded number of sensors in a network
  - Dynamic topology
  - Unbounded Intruder behavior
  - Formal proofs are expensive
- Approach:
  - Put a bound on number of sensors
  - Verify against all possible topologies for bounded number of sensors, one at a time
  - Provide intruder with information about protocol to bind behavior

Overview
- Automatically extracts models from source code
- Translated the generated counterexample written in PROMELA to the corresponding statements sequence int nesC
- Provides extensibility by verifying against different intruders (node compromise, Dolev-Yao, etc.)
- Generated intruder model is merged into the protocol model

Automatically extracts models from source code

Program analysis based optimizations to enhance scalability

Given a bounded number of sensors, all possible topologies are generated for thorough verification

Information about messages exchanged in the protocol that is required for the intruder to make smart attacks

Goals written in terms of commands/events (functions) of the implementation for easier specification of goals

Translated the generated counterexample written in PROMELA to the corresponding statements sequence int nesC

Goals written in terms of commands/events (functions) of the implementation for easier specification of goals

Provides extensibility by verifying against different intruders (node compromise, Dolev-Yao, etc.)

Generated intruder model is merged into the protocol model

nesC code for protocol

Annotation

Topology

Message Structure Mapping

Verification Goals

Protocol Model Generator

Intruder Model Generator

Intruder Library

SPIN

Counterexample Translator

Sliede

Specification and verification of Sensor Networks Security Protocols

Overview

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, Connecticut